Abstract

In some network configurations, it is desirable for the end system to be able to obtain its geodetic or civic location using an application-layer protocol. This document describes RELO; a simple, HTTP-based stateless protocol that fulfills this need.
Table of Contents

1. Introduction ............................................. 3
2. Terminology ................................................ 3
3. Overview .................................................. 3
   3.1 Discovery .............................................. 3
   3.2 Query ................................................ 4
   3.3 Response .............................................. 4
4. XML Schema Definition ..................................... 6
5. IANA Considerations ....................................... 7
6. Security Considerations ................................... 9
7. Acknowledgments .......................................... 10
8. References ................................................ 10
   8.1 Normative References .................................. 10
   8.2 Informative References ................................ 11
Author’s Address ............................................. 11
Intellectual Property and Copyright Statements .............. 12
1. Introduction

The RELO protocol allows end systems (devices) to obtain information about their current geodetic (longitude, latitude) or civic (jurisdictional or postal street address) location, based on their Internet Protocol address or possibly other identifiers. The protocol uses HTTP [3] to retrieve the information. The location information can be returned by value or by reference, either for retrieval or for event notification by subscription.

The protocol is motivated by the requirement that end user network-layer equipment, such as DSL modems, routers, NATs and wireless access points, cannot be modified. Hence, a DHCP or PPP based solution cannot be reused. A more detailed problem statement is provided in [11]. To reduce privacy risks, RELO is designed for "first-party" retrieval, i.e., the device obtains its own location or a reference thereto. It is not designed for a third party to retrieve location information about a device. However, RELO may retrieve a reference to location information that can be passed to third parties.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].


3. Overview

This section describes the Location Information Server (LIS) discovery procedure (see Section 3.1), the query message (see Section 3.2) and the response message (see Section 3.3).

3.1 Discovery

The URI for the location server is conveyed via DNS (S-NAPTR) [8]. The domain is determined from the domain name of the end host, typically conveyed as part of the configuration information or obtainable from the public IP address via DNS PTR records.

```plaintext
dhcp-17.example.com.
; order pref flags service regexp
IN NAPTR 50 50 "a" "Location.relo" "*
; replacement
relo.example.org
```
3.2 Query

The query is transmitted to the server in an HTTP GET request, using the media type application/relo+xml. The use of TLS [10] is RECOMMENDED.

The end system is identified by default by its IP address, contained in the IP packets carrying the HTTP request. If the querier is behind a NAT or firewall, the server will see the querier’s public IP address and use that address to identify the end system. In those cases, the location of the network termination equipment, such as the DSL modem or 802.11 access point, will be returned, not the actual location of the querier since the LIS generally has no way to estimate that location. Other identifiers, such as switch and port information, are for further study.

The format of the location information is contained in the <by> element of the query and can indicate that either civic or geo(spatial) information is desired and whether the client wishes to obtain the value ("value"), a reference to the current value ("reference") or a subscription to change notifications for the value ("events"). A query example is shown below:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<get-location by="value" type="civic"
  xmlns="urn:ietf:params:xml:ns:relo1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" />
```

This protocol does not provide the ability for the end host to transmit a location estimate as, for example, obtained from a local GPS receiver, to the LIS.

3.3 Response

A successful response contains the civic and or geospatial location information related to the identifier of the querier. Note that this proposal does not return a PIDF-LO [12] since most of the values carried by the PIDF-LO cannot be meaningfully instantiated by the network without the help of the end host. This proposal allows the end host to instantiate the values by itself without introducing security challenges and privacy risks. If the querier indicated a preference for location-by-reference, the answer simply contains a URI-list, i.e., media type text/uri-list [2].

Normal HTTP status responses are used to indicate failure conditions, e.g., when the information is unavailable.
The server indicates the validity period of the information using the HTTP Expires header field. If a reference is returned, the reference URL itself is not guaranteed to be valid beyond the expiration time.

The server MAY provide one or more URLs in a new HTTP header field, Subscribe, that the client can subscribe to if it wants to receive updates for the object retrieved via HTTP. At least one of the URLs MUST be a SIP URL. For SIP, the event name to be used in the subscription can be encoded in the URL. (An HTTP header field was chosen since the subscription mechanism does not depend on the media type and also applies to media types that would make it difficult to embed such subscription URLs, such as a JPEG image.) The server makes no guarantees that the client has the appropriate credentials to subscribe to the object. Clients MAY support this mechanism; all clients that do support subscriptions MUST support the SIP SUBSCRIBE and NOTIFY methods.

The field value consists of one or more absolute URIs:

```
Subscribe = "Subscribe" ":" 1#absoluteURI
```

An example is:

```
Subscribe: sip:data@example.com?Event=location
```

[TBD: Since this mechanism is not limited to location delivery, this might be better separated into a stand-alone draft.]

The response containing the location information is not signed.

Response message examples are shown below starting with a response providing geospatial location information and followed by civic location information. Finally, we show an example with location-by-referency.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<returnlocation xmlns="urn:ietf:params:xml:ns:relo1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:gml="http://www.opengis.net/gml">
  <gml:location>
    <gml:Point gml:id="point1" srsName="epsg:4326">
    </gml:Point>
  </gml:location>
</returnlocation>
```
<returnlocation xmlns="urn:ietf:params:xml:ns:relo1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
<civilAddress>
<p2:country>Deutschland</p2:country>
<p2:A1>Bayern</p2:A1>
<p2:A3>Muenchen</p2:A3>
<p2:A6>Neu Perlach</p2:A6>
<p2:HNO>96</p2:HNO>
<p2:PC>81675</p2:PC>
</civilAddress>
</returnlocation>

<returnURI xmlns="urn:ietf:params:xml:ns:relo1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<URI>sip:15555551002adfkfjyongqoiyukjgkly@example.com</URI>
</returnURI>

4. XML Schema Definition

This section provides the XML schema.
<simpleType name="byType">
   <restriction base="string">
      <enumeration value="value"/>
      <enumeration value="reference"/>
   </restriction>
</simpleType>

<!-- Responses -->
<element name="result" abstract="true"/>

<element name="returnlocation" type="relo:returnlocationType"
   substitutionGroup="relo:result"/>
<complexType name="returnlocationType">
   <complexContent>
      <restriction base="anyType">
         <sequence>
            <element ref="gml:location" minOccurs="0"
               maxOccurs="1"/>
            <element name="civilAddress"
               type="civilLoc:civilAddress"
               minOccurs="0" maxOccurs="1"/>
         </sequence>
      </restriction>
   </complexContent>
</complexType>

<element name="returnURI" type="relo:returnURIType"
   substitutionGroup="relo:result"/>
<complexType name="returnURIType">
   <sequence>
      <element name="URI" type="anyURI" minOccurs="1"
         maxOccurs="1"/>
   </sequence>
</complexType>
</schema>

5. IANA Considerations

This document registers the label "RELO" as the S-NAPTR application service tag according to [8] for location lookup services and defines the intended usage, interoperability considerations and security considerations (Section 6).

This document requests the registration of a new message header field, 'Subscribe', according to RFC 3864 [7].
Header field name: Subscribe

This specification also requests the registration of a new MIME type according to the procedures of [RFC 4288] and guidelines in [RFC 3023].

MIME media type name: application

MIME subtype name: relo+xml

Mandatory parameters: none

Optional parameters: charset

Indicates the character encoding of enclosed XML.

Encoding considerations:

Uses XML, which can employ 8-bit characters, depending on the character encoding used. See [RFC 3023], Section 3.2.

Security considerations:

This content type is designed to carry authorization policies. Appropriate precautions should be adopted to limit disclosure of this information. Please refer to Section 6 of RFCXXXX [NOTE TO IANA/RFC-EDITOR: Please replace XXXX with the RFC number of this specification.] and to the security considerations described in Section 10 of RFC 3023 [4] for more information.

Interoperability considerations: None

Published specification: RFCXXXX [NOTE TO IANA/RFC-EDITOR: Please replace XXXX with the RFC number of this specification.] this document

Applications which use this media type:

Presence- and location-based systems

Additional information:

Magic Number: None
6. Security Considerations

If IP addresses are used as identifiers, RELO relies on return routability to ensure that only the current owner of an IP address can obtain location information for that host, and assumes that an attacker cannot generate and intercept packets for a spoofed IP address. Note that TLS itself does not prevent client address spoofing if the attacker can intercept and generate IP packets with the victim’s IP address.

The victim can be protected against this privacy breach if the client and LIS share a secret, such as a username/password combination, and the LIS can associate an IP address with a particular user, e.g., based on PPP authentication. In that case, HTTP digest authentication can be used to prevent a third party from using a spoofed IP address to fraudulently obtain location information. Unfortunately, such authentication information is not generally available to wireless nodes in residential networks, for example.

To prevent others from accessing location information for a particular host, the reference to a Location Object MUST NOT be guessable. For example, it may contain a random component. It is RECOMMENDED to use TLS with confidentiality protection to prevent eavesdroppers to observe the protocol exchange between the end host and the LIS.

Signing of location information is beyond the scope of this document [TBD; if desired, reference to other document, since this is not specific to obtaining location information]. Thus, colluding attackers may be able to obtain and replay location information that does not correspond to their true location.
7. Acknowledgments

This document is based on discussions with Hannes Tschofenig and inspired by protocols such as HELD.

8. References

8.1 Normative References


Informative References


Author’s Address

Henning Schulzrinne
Columbia University
Department of Computer Science
450 Computer Science Building
New York, NY 10027
US
Phone: +1 212 939 7004
Email: hgs+geopriv@cs.columbia.edu
URI: http://www.cs.columbia.edu
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2006). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.